Abgeordnetenhaus BERLIN

Drucksache 18 / 16 159
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Adrian Grasse (CDU)

vom 27. August 2018 (Eingang beim Abgeordnetenhaus am 30. August 2018)

zum Thema:
Cybersicherheit an Berlins Hochschulen

und **Antwort** vom 14. September 2018 (Eingang beim Abgeordnetenhaus am 18. Sep. 2018)

Der Regierende Bürgermeister von Berlin
Senatskanzlei - Wissenschaft und Forschung -

Herrn Abgeordenten Adrian Grasse (CDU)

über

den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 18/16 159
vom 27. August 2018
über Cybersicherheit an Berlins Hochschulen

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Die Anfrage betrifft Sachverhalte, die der Senat nicht ohne Beiziehung der Hochschulen beantworten kann. Es wurden die staatlichen Berliner Hochschulen um Stellungnahme gebeten.

Vor wenigen Tagen wurde bekannt, dass Cyberangriffe auf Bundesbehörden in Berlin aus dem Ausland unternommen wurden und werden. Diese Angriffe haben auch dazu geführt, dass der Lehrbetrieb bzw. das Onlinelehrangebot der Bundesfachhochschule (u. a. für den Bereich Sozialversicherungen in Berlin) eingeschränkt werden musste. Angesichts des Umstands, dass die Berliner Hochschulen über zahlreiche Personendaten, einschließlich Prüfungsergebnisse verfügen, frage ich den Senat:

1. Wie viele Hackerangriffe wurden in den letzten fünf Jahren gegen Berliner Hochschulen unternommen? Welche Hochschulen waren besonders betroffen?

Zu 1.:
Grundsätzlich ist anhand der Antworten der Hochschulen, welche entsprechende Erhebungen durchführen können, zu erkennen, dass alle Hochschulen zumindest in Bezug auf Hackerangriffe (im weitesten Sinne, wenn allein schon der Versuch ein Angriff ist) gleichermaßen betroffen sind. Dies liegt daran, dass zum größten Teil von automatisierten Angriffen auszugehen ist. Diese testen die IT-Systeme automatisch auf Sicherheitslücken und Schwachstellen. Zudem ist zu differenzieren, ob es sich um interne Netze handelt oder z.B. lediglich um Webpräsenzen. Gerade Letztere waren mehrfach Ziel von Hack-Versuchen, obwohl diese Systeme zum Teil bei Externen gehostet werden, d.h. die Informationen zu den Webpräsenzen liegen auf externer Hardware und die IT-Sicherheit der Externen ist zuständig. Bei den Zugriffen auf interne Netze, handelt es sich um Versuche, unsichere Server und/oder Arbeitsplatzcomputer zu finden und zu kapern oder per E-Mail-Schadsoftware (über Phishing oder Trojaner) im Hochschulnetz einzuschleusen und zu verbreiten. Dabei handelt es sich teilweise um die in der Presse diskutierten „dDos-

Attacken“. Bei Log-In Versuchen (ob automatisch oder manuell) kommt für eine Bewertung erschwerend hinzu, dass die sog. Logs nur temporär gespeichert werden. Somit kann in Bezug auf die Frage hierzu keine quantitativ valide Antwort gegeben werden.

2. Wie viele dieser Angriffe konnten abgewehrt werden und wie viele waren erfolgreich?

Zu 2.:
In der Summe ist festzustellen, dass trotz der zahlreichen Angriffs-Versuche (durch die automasierten Attacken), nur eine verschwindend geringe Anzahl an erfolgreichen Versuchen zu verzeichnen ist. Der Beuth-Hochschule für Technik Berlin (Beuth) sind zwei erfolgreiche Angriffe bekannt. An der Technischen Universität Berlin (TU) sind sieben erfolgreiche Angriffe verzeichnet worden. An der Hochschule für Musik „Hanns Eisler“ (HfM) war ein Angriff auf die Webseite erfolgreich, abgewehrt wurde keiner. Bei der Hochschule für Wirtschaft und Recht (HWR) war ein Hack Anfang 2013 auf den Webserver erfolgreich. Zudem wurden zwei HWR-Accounts übernommen und für das Verschicken von Spam-E-Mails missbraucht. An der „Alice-Salomon“-Hochschule für Sozialarbeit und Sozialpädagogik Berlin (ASH) sind fünf erfolgreiche Angriffe bekannt geworden.

3. Welche Schäden sind durch erfolgreiche Angriffe entstanden? Welcher Typ an Daten konnte von den Angreifern erbeutet werden?

Zu 3.:
Beuth: Das Hochschulrechenzentrum der Beuth vermutet aufgrund der Art eines erkannten Angriffs, dass Apple-Logins durch externe Personen erbeutet werden konnten. Eine genaue Zahl war nicht feststellbar. Zudem erhält die Beuth gelegentlich Informationen über Account-Daten, die in die Hände Dritter gelangt sind, bzw. es werden Accounts erkannt, die missbräuchlich durch Dritte verwendet werden. Eine genaue Anzahl liegt nicht vor. Nach Schätzungen der Beuth handelt es sich um eine Zahl im unteren zweistelligen Bereich.

HfM: Bei der HfM wurde die Startseite überschrieben, ansonsten ist kein Schaden entstanden.

Kunsthochschule Berlin (Weißensee) – Hochschule für Gestaltung (KHB): Bei der KHB ist die Startseite überschrieben worden, ansonsten ist kein Schaden entstanden.

TU: Einzelne mittelschwere Fälle betrafen die TU.
(1) So handelte es sich in einem der Fälle um einen „dDos-Angriff“, bei dem allerdings keine Daten erbeutet wurden. Als Schaden war die Website der TU für ca. sieben Stunden nicht erreichbar.
(2) Ein anderer Fall betraf eine Sicherheitslücke des „Domain Name Service“ (DNS), welche für einen „DNS-Reflection-DOS-Angriff“ ausgenutzt wurde. Der „DNS“ wurde auf Grund einer Sicherheitslücke als Zwischenstation benutzt, um eine „DOS-Attacke“ aufzubauen. D.h. die IT-Infrastruktur der TU wurde dafür genutzt, einen Angriff auf andere Strukturen durchzuführen. Ob die Attacke erfolgreich war, kann von der TU nicht beantwortet werden, da sie nicht das Ziel dieser Attacke war. Es wurden keine Daten erbeutet.
(3) In einem weiteren Fall erfolgte ein Angriff über einen gehackten Dienst-Account für eine Mailinglistensoftware, der erfolgreich auf mehreren Systemen mit einem Apple MacOS Betriebssystem einen „IRC-Bouncer“ (Proxy für einen „IRC-Dienst“) aufsetzen konnte. Der Schaden entstand hier durch die kompromittierten Clientrechner, die für eine „dDOS-Attacke“ ausgenutzt werden konnten. Über den Erfolg einer solchen „dDOS-Attacke“ können keine Angaben gemacht werden, da die TU selbst nicht das Ziel der

Attacke waren. Da der Angriff automatisiert aufgebaut war, geht die TU davon aus, dass keine weiteren Daten erbeutet wurden. Die kompromittierten Clientrechner wurden neu installiert.
(4) In zwei Fällen erfolgten zwei erfolgreiche Phishing-Angriffe (je ein einzelner Useraccount). Die erbeuteten Mailzugangsdaten wurden in beiden Fällen ausgenutzt, um Massen-Spam-E-Mails zu verschicken. Es wurden keine weiteren Daten erbeutet. In einem weiteren Fall wurde eine Sicherheitslücke am Webmailer für den Massenmailversand ausgenutzt, um Massen-Spam-E-Mails zu verschicken.

ASH: Bei der ASH handelte es sich in allen Fällen um übernommene Mailaccounts, die zum massiven Spamversand missbraucht wurden. Es bestand Zugriff auf Mailadressen und die Inhalte der Mailpostfächer. Der verursachte Schaden bestand im Wesentlichen in einer zeitweisen Beeinträchtigung der Nutzbarkeit des Mailsystems der ASH.

4. Welche Erkenntnisse liegen dem Senat über die Angreifer vor?

Zu 4.:
Dem Senat liegen in fast allen Fällen keine Erkenntnisse über die Angreiferinnen bzw. Angreifer vor. Nur bei der TU hat die Rückverfolgung der Angreifer-IPs ergeben, dass es sich um ein „BOT-Netz“ mit mehrheitlich chinesischen IPs handelte (erster Fall unter Frage 3). Im drittgenannten Fall unter 3. wurde ermittelt, dass diverse IPs aus .net und .com sowie aus dem rumänischen Domainbereich .ro verwendet wurden. Bei den beiden viertgenannten Fällen konnte für einen Fall ein Absender einer Phishingmail aus Lagos (Nigeria) ermittelt werden, für den zweiten liegen keine Erkenntnisse vor. Im sechstgenannten Fall wurde das betroffene System zur Versendung von Phishing Mails genutzt, die auf Täterinnen bzw. Täter aus dem Umfeld der organisierten Kriminalität schließen ließen, deren Vorgehensmodell die Vermietung von kompromittierten Computerressourcen ist.

5. Welche Strategien verfolgen die Hochschulen zur Abwehr solcher Angriffe? Gibt es hier eine hochschulübergreifende Kooperation und/oder gemeinsame Krisenabwehrvorkehrungen?

Zu 5.:
Die Hochschulen tauschen sich nicht nur untereinander, sondern auch mit externen Netzwerken und Informationsdiensten aus bzw. bedienen sich einschlägiger Informationsquellen bzgl. aktueller Entwicklungen.

Ein Großteil der Hochschulen nutzt die Möglichkeiten im Rahmen des Deutschen Forschungsnetzes (DFN). Diese beinhalten: Inanspruchnahme von verschiedenen Warndiensten des DFN, Teilnahme an Betriebstagungen sowie die Zusammenarbeit der „Computer Emergency Response Teams“ (CERT) der Mitgliedseinrichtungen. Zudem nehmen die Hochschulen an regelmäßig stattfindenden Erfahrungsaustauschen von IT-Sicherheitsbeauftragten deutscher Hochschulen teil. Einzelne Hochschulen sind Mitglieder im Arbeitskreis IT-Sicherheit der Zentren für Kommunikationsverarbeitung in Forschung und Lehre (ZKI). Bedarfsweise werden Kooperationen mit staatlichen Einrichtungen (Verfassungsschutz, Bundeskriminalamt) und weiteren Partnern eingegangen. Die Hochschulen orientieren sich des Weiteren an den Richtlinien und entsprechender Empfehlungen bzgl. Maßnahmen des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bei den kleineren Berliner Hochschulen werden Synergieeffekte angestrebt: Das „ServiceCenter IT“ (SC-IT) betreut als gemeinsame Einrichtung die Netze der HfM, der Hochschule für Schauspielkunst "Ernst Busch" (HfS) und der KHB. Es wird moderne Hardware für die Netzwerke eingesetzt, eine professionelle Netzwerkinfrastruktur und aktuelle siche-

re Firewalls. Für die Abwehr von Angriffen wird professionelle Software eingesetzt, sowohl ein „Intrusion Detection System“ auf der Firewall, als auch Antivirensoftware und eine Schnittstellenkontrolle am „APC“. Zudem wird eine Benutzerverwaltung verwendet, die nur der jeweiligen Benutzerin bzw. dem jeweiligen Benutzer die notwendigen Rechte gewährt. Die Kommunikation zwischen den Standorten der Hochschulen erfolgt verschlüsselt. Wichtige Dienste sind an professionelle Anbieter ausgelagert.

Grundsätzlich werden als weitere Einzelmaßnahmen an einzelnen Hochschulen die Benennung von IT-Sicherheitsmitarbeiterinnen und Sicherheitsmitarbeitern, sowie Datenschutzbeauftragten genannt. Zudem bedarf es für eine Breitenwirkung einer kontinuierlichen Sensibilisierung aller mit IT-Infrastruktur befassten Mitarbeiterinnen und Mitarbeiter. Hierfür dienen auch verbindliche Regelwerke (z.B. an der FU) und es werden Absprachen zwischen zentralen und dezentralen IT-Infrastrukturen getroffen (TU). In speziellen Fällen wie an der Charité – Universitätsmedizin Berlin (Patientendaten und kritische Infrastruktur) sind kritische Systeme grundsätzlich nicht direkt aus dem Internet erreichbar. Für aus dem Internet erreichbare Systeme, bzw. exponierte Dienste sind über den üblichen Schutz hinaus besondere Maßnahmen und Verfahren etabliert. Die Universität der Künste (UdK) trennt die sensiblen Netzbereiche der Verwaltung nicht nur logisch, sondern physisch voneinander: Es wurde zum Schutz der sensiblen Systeme und Daten der Aufbau mit mehrere separaten „Demilitarisierten Zonen“ (DMZ) gewählt. Diese sind teilweise mehrstufig aufgebaut. Der Zugriff erfolgt über Proxy-Systeme. Die Beuth hat in der Vergangenheit ein IT Sicherheitskonzept extern in Auftrag gegeben, das auf dem BSI Grundschutzkatalog basiert.

6. Wie viele Personen (bzw. Vollzeitäquivalente) sind an den Hochschulen in diesem Bereich beschäftigt?

Zu 6.:
Die Zählung der klar zuordenbaren Stellenprofile zu diesem Thema ergab berlinweit eine Anzahl von 39 Mitarbeiterinnen und Mitarbeiter. Darüber hinaus sind in diesem Bereich unterschiedliche Personen auf unterschiedlichen Ebenen für die Thematik der IT-Sicherheit zuständig bzw. verantwortlich.

7. Inwieweit unterstützen der Senat bzw. die Senatsverwaltung und die Berliner Sicherheitsbehörden die Hochschulen beim Ausbau der Cybersicherheit?

Zu 7.:
Die Berliner Datenschutzbeauftragte fungiert als berlinweite Anlaufstelle zu Fragen des Datenschutzes. Es kann jedoch festgestellt werden, dass die aktuelle Situation bzgl. der Cybersicherheit an den Berliner Hochschulen durch die diversen dargestellten Maßnahmen sehr gut ist und in Relation zu der Größe und Anzahl der Hochschulen in Berlin nur wenige Fälle von Cyber-Kriminalität auftraten.

Berlin, den 14. September 2018

In Vertretung
Steffen Krach
Der Regierende Bürgermeister von Berlin
Senatskanzlei - Wissenschaft und Forschung -